(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-46460
(P2004-46460A)
(43)公開日　平成16年2月12日(2004.2.12)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330D	5B017
G06F 12/00	G06F 12/00	537A	5B082
G06F 12/14	G06F 12/14	310K	5B085
H04L 12/66	H04L 12/66	B	5K030

審査請求 未請求　請求項の数 6　OL　（全 12 頁）

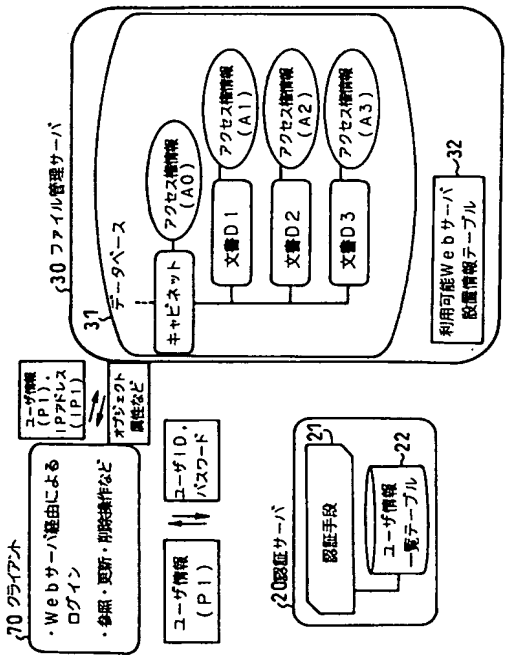
(21)出願番号　特願2002-201872(P2002-201872)
(22)出願日　平成14年7月10日(2002.7.10)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100088890
弁理士　河原　純一
(72)発明者　伊藤　秀俊
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B017 AA03 AA07 BA05 BA06 BB06
BB10 CA16
5B082 EA11 EA12 GA13
5B085 AA08 AE02 AE06 AE15 AE23
BC02 BG02 BG07 CA02 CA04
5K030 GA15 HA08 HC01 HC13 HD03
KA04 LD19

(54)【発明の名称】ファイル管理システムにおけるアクセス制御方式

(57)【要約】
【課題】同一ユーザによる同一オブジェクトへのアクセスであっても、社内・社外どちらからのアクセスかに応じて、異なるアクセス権を設定可能とする。
【解決手段】クライアント７０は、キャビネット，文書等のオブジェクトへのアクセス時にユーザ情報およびログイン時に経由したＷｅｂサーバのＩＰアドレスをファイル管理サーバ３０に渡す。ファイル管理サーバ３０は、利用可能Ｗｅｂサーバ設置情報テーブル３２に登録されているＩＰアドレスに対応する設置情報を取得し、ユーザ情報および設置情報をキーとしてオブジェクトのアクセス権情報を検索してユーザのオブジェクトへのアクセス権の有無を判定する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
Ｗｅｂベースのファイル管理システムにおいて、
クライアントからファイル管理サーバへのログインの要求時に、クライアントから受け取ったユーザＩＤがユーザ情報一覧テーブルに登録されているかどうかをチェックし、ユーザＩＤが登録されていたならばクライアントから受け取ったパスワードが前記ユーザ情報一覧テーブルにユーザＩＤに対応して登録されているパスワードと一致するかどうかをチェックし、パスワードが一致した場合には前記ユーザ情報一覧テーブルから該当ユーザのユーザ情報を取得してクライアントに返却する認証サーバと、
対象オブジェクトを示すインスタンスＩＤ，前記認証サーバから得られたユーザ情報，およびログイン時に経由したＷｅｂサーバのＩＰアドレスを前記ファイル管理サーバに渡すクライアントと、
オブジェクト，およびオブジェクト毎のアクセス権情報を登録するデータベースと、利用可能Ｗｅｂサーバ設置情報テーブルとを備え、クライアントからのオブジェクトへのアクセス要求があったときに、前記利用可能Ｗｅｂサーバ設置情報テーブルから前記ＩＰアドレスに対応する設置情報を取得し、ユーザ情報および設置情報をキーとして対象オブジェクトのアクセス権情報を検索してユーザの対象オブジェクトへのアクセス権の有無を判定し、ユーザが対象オブジェクトへのアクセス権を有しているときにオブジェクトにアクセスし、アクセス結果を前記クライアントに送信するファイル管理サーバと
を有することを特徴とするファイル管理システムにおけるアクセス制御方式。
【請求項２】
前記アクセス権情報が、少なくとも、ユーザを示す要求元と、ログイン時に経由したＷｅｂサーバがファイアウォールの内に存在するか外に存在するかを示す設置情報と、ユーザのオブジェクトへのアクセス権の有無とを含むことを特徴とする請求項１記載のファイル管理システムにおけるアクセス制御方式。
【請求項３】
前記利用可能Ｗｅｂサーバ設置情報テーブルが、ＷｅｂサーバのＩＰアドレスと、Ｗｅｂサーバがファイアウォールの内に存在するか外に存在するかを示す設置情報とを含むことを特徴とする請求項１記載のファイル管理システムにおけるアクセス制御方式。
【請求項４】
クライアントがファイル管理サーバへのログイン時に認証サーバから認証結果としてユーザ情報を取得するとともに経由したＷｅｂサーバのＩＰアドレスを取得する工程と、
クライアントがオブジェクトへのアクセス要求時に前記ユーザ情報および前記ＩＰアドレスをファイル管理サーバに渡す工程と、
ファイル管理サーバが利用可能Ｗｅｂサーバ設置情報テーブルに前記ＩＰアドレスが登録されているかどうかを判定する工程と、
前記ＩＰアドレスが登録されているときにファイル管理サーバが前記利用可能Ｗｅｂサーバ設置情報テーブルから前記ＩＰアドレスに対応する設置情報を取得する工程と、
ファイル管理サーバがユーザ情報および設置情報をキーとして対象オブジェクトのアクセス権情報を検索しユーザのオブジェクトへのアクセス権の有無を判定する工程と、
ユーザがオブジェクトへのアクセス権を有しているときにファイル管理サーバが対象オブジェクトにアクセスしてアクセス結果をクライアントに送信する工程と、
クライアントがファイル管理サーバからオブジェクトのアクセス結果を受信する工程と
を含むことを特徴とするファイル管理システムにおけるアクセス制御方法。
【請求項５】
コンピュータに、ファイル管理サーバへのログイン時に認証サーバのから認証結果としてユーザ情報を取得するとともに経由したＷｅｂサーバのＩＰアドレスを取得する工程と、
オブジェクトへのアクセス要求時に前記ユーザ情報および前記ＩＰアドレスをファイル管理サーバに渡す工程と、ファイル管理サーバからオブジェクトのアクセス結果を受信する工程とを実行させるためのプログラム。

【請求項６】
コンピュータに、利用可能Ｗｅｂサーバ設置情報テーブルを参照してＩＰアドレスが登録されているかどうかを判定する工程と、前記ＩＰアドレスが登録されているときに前記利用可能Ｗｅｂサーバ設置情報テーブルから前記ＩＰアドレスに対応する設置情報を取得する工程と、ユーザ情報および設置情報をキーとしてアクセス権情報を検索しユーザのオブジェクトへのアクセス権の有無を判定する工程と、ユーザがオブジェクトへのアクセス権を有しているときにオブジェクトにアクセスし、アクセス結果をクライアントに送信する工程とを実行させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はファイル管理システムにおけるアクセス制御方式に関し、特にＷｅｂベースのファイル管理システムにおける社内・社外ログイン時のアクセス制御方式に関する。
【０００２】
【従来の技術】
今日では、インターネット等の技術進歩により社内・社外を問わず、また会社間の垣根を越えた共通のワークスペース（コーポレートウェアなど）が提供されており、そのニーズも拡大している。このように、ファイル管理システムなどにおけるシームレス化が進む一方で、セキュリティ面での強化がますます要求されている。
【０００３】
ところで、従来のファイル管理システムにおけるアクセス制御方法としては、端末グループによってアクセス権を異ならしめたり（特開平０２－２８２８４２参照）、時間帯に応じてアクセスの妥当性を変化させたり（特開平０２－２８５４３９参照）、プレゼンテーションの内容を使用者によって抑止させたり（特開平０３－１５４９６９参照）する各種の方法が知られていた。
【０００４】
【発明が解決しようとする課題】
しかし、従来の技術では、ユーザが、社内からキャビネット，フォルダ，文書（ドキュメント）などのオブジェクトにアクセスする場合でも、社外からオブジェクトにアクセスする場合でも、同じセキュリティのレベルであり、特に社外からオブジェクトにアクセスする場合には社内からオブジェクトにアクセスする場合に比べてセキュリティ面での強化を行いたいという要請があっても行えないという問題点があった。その理由は、ファイル管理サーバでは、キャビネット，フォルダ，文書などのオブジェクト単位で権利認証（Ａｕｔｈｏｒｉｚａｔｉｏｎ）に利用されるアクセス権を設定可能であったが、同一ユーザが社内から同一オブジェクトにアクセスした場合でも、社外から同一オブジェクトにアクセスした場合でも、オブジェクトに設定されるアクセス権情報が同じであったからである。
【０００５】
本発明の目的は、Ｗｅｂベースのファイル管理システムにおいて、同一ユーザからの同一オブジェクトへのアクセスについて、社内からのアクセスであるか社外からのアクセスであるかに応じて、異なるアクセス権を設定可能なファイル管理システムにおけるアクセス制御方式を提供することにある。
【０００６】
また、本発明の他の目的は、Ｗｅｂベースのファイル管理システムにおいて、同一ユーザによる同一オブジェクトへのアクセスであっても、社内からのアクセスであるか社外からのアクセスであるかに応じて、権利認証を異ならしめるようにしたファイル管理システムにおけるアクセス制御方法を提供することにある。
【０００７】
【課題を解決するための手段】
本発明のファイル管理システムにおけるアクセス制御方式は、Ｗｅｂベースのファイル管理システムにおいて、クライアントからファイル管理サーバへのログインの要求時に、ク

ライアントから受け取ったユーザＩＤがユーザ情報一覧テーブルに登録されているかどうかをチェックし、ユーザＩＤが登録されていたならばクライアントから受け取ったパスワードが前記ユーザ情報一覧テーブルにユーザＩＤに対応して登録されているパスワードと一致するかどうかをチェックし、パスワードが一致した場合には前記ユーザ情報一覧テーブルから該当ユーザのユーザ情報を取得してクライアントに返却する認証サーバと、対象オブジェクトを示すインスタンスＩＤ，前記認証サーバから得られたユーザ情報，およびログイン時に経由したＷｅｂサーバのＩＰアドレスを前記ファイル管理サーバに渡すクライアントと、オブジェクト，およびオブジェクト毎のアクセス権情報を登録するデータベースと、利用可能Ｗｅｂサーバ設置情報テーブルとを備え、クライアントからのオブジェクトへのアクセス要求があったときに、前記利用可能Ｗｅｂサーバ設置情報テーブルから前記ＩＰアドレスに対応する設置情報を取得し、ユーザ情報および設置情報をキーとして対象オブジェクトのアクセス権情報を検索してユーザの対象オブジェクトへのアクセス権の有無を判定し、ユーザが対象オブジェクトへのアクセス権を有しているときにオブジェクトにアクセスし、アクセス結果を前記クライアントに送信するファイル管理サーバとを有することを特徴とする。

【０００８】

また、本発明のファイル管理システムにおけるアクセス制御方式は、前記アクセス権情報が、少なくとも、ユーザを示す要求元と、ログイン時に経由したＷｅｂサーバがファイアウォールの内に存在するか外に存在するかを示す設置情報と、ユーザのオブジェクトへのアクセス権の有無とを含むことを特徴とする。

【０００９】

さらに、本発明のファイル管理システムにおけるアクセス制御方式は、前記利用可能Ｗｅｂサーバ設置情報テーブルが、ＷｅｂサーバのＩＰアドレスと、Ｗｅｂサーバがファイアウォールの内に存在するか外に存在するかを示す設置情報とを含むことを特徴とする。

【００１０】

一方、本発明のファイル管理システムにおけるアクセス制御方法は、クライアントがファイル管理サーバへのログイン時に認証サーバから認証結果としてユーザ情報を取得するとともに経由したＷｅｂサーバのＩＰアドレスを取得する工程と、クライアントがオブジェクトへのアクセス要求時に前記ユーザ情報および前記ＩＰアドレスをファイル管理サーバに渡す工程と、ファイル管理サーバが利用可能Ｗｅｂサーバ設置情報テーブルに前記ＩＰアドレスが登録されているかどうかを判定する工程と、前記ＩＰアドレスが登録されているときにファイル管理サーバが前記利用可能Ｗｅｂサーバ設置情報テーブルから前記ＩＰアドレスに対応する設置情報を取得する工程と、ファイル管理サーバがユーザ情報および設置情報をキーとして対象オブジェクトのアクセス権情報を検索しユーザのオブジェクトへのアクセス権の有無を判定する工程と、ユーザがオブジェクトへのアクセス権を有しているときにファイル管理サーバが対象オブジェクトにアクセスしてアクセス結果をクライアントに送信する工程と、クライアントがファイル管理サーバからオブジェクトのアクセス結果を受信する工程とを含むことを特徴とする。

【００１１】

他方、本発明のプログラムは、コンピュータに、ファイル管理サーバへのログイン時に認証サーバのから認証結果としてユーザ情報を取得するとともに経由したＷｅｂサーバのＩＰアドレスを取得する工程と、オブジェクトへのアクセス要求時に前記ユーザ情報および前記ＩＰアドレスをファイル管理サーバに渡す工程と、ファイル管理サーバからオブジェクトのアクセス結果を受信する工程とを実行させることを特徴とする。

【００１２】

また、本発明のプログラムは、コンピュータに、利用可能Ｗｅｂサーバ設置情報テーブルを参照してＩＰアドレスが登録されているかどうかを判定する工程と、前記ＩＰアドレスが登録されているときに前記利用可能Ｗｅｂサーバ設置情報テーブルから前記ＩＰアドレスに対応する設置情報を取得する工程と、ユーザ情報および設置情報をキーとしてアクセス権情報を検索しユーザのオブジェクトへのアクセス権の有無を判定する工程と、ユーザ

がオブジェクトへのアクセス権を有しているときにオブジェクトにアクセスし、アクセス結果をクライアントに送信する工程とを実行させることを特徴とする。

【００１３】

本発明は、ファイル管理サーバへのログイン時に経由する社内Ｗｅｂサーバまたは社外Ｗｅｂサーバの設置情報（ファイアウォール内・外の情報）を、ファイル管理サーバで行う権利認証の中で利用することを特徴とするものである。ユーザがクライアントから社内Ｗｅｂサーバを経由してファイル管理サーバにログインした場合にはアクセス対象のオブジェクト（以下、対象オブジェクトという）にアクセスすることができる一方、クライアントから社外Ｗｅｂサーバを経由してファイル管理サーバにログインした場合には対象オブジェクトにアクセスすることができないようにすることができる。このため、Ｗｅｂサーバの設置情報を、そのままユーザからのファイル管理サーバへのアクセス権情報の一部として利用する。

【００１４】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

【００１５】

［第１の実施の形態］

図２は、本発明の第１の実施の形態に係るアクセス制御方式が適用されるファイル管理システムのシステム構成図である。このファイル管理システムは、ローカルエリアネットワーク（ＬＡＮ）等でなる社内ネットワーク１０と、社内ネットワーク１０に接続された認証サーバ２０と、社内ネットワーク１０に接続されたファイル管理サーバ３０と、社内ネットワーク１０に接続されたＷｅｂサーバ（以下、社内Ｗｅｂサーバという）４０と、社内ネットワーク１０に接続されたファイアウォール５０と、ファイアウォール５０およびインターネット等の外部回線に接続されたＷｅｂサーバ（以下、社外Ｗｅｂサーバという）６０と、社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０を経由してファイル管理サーバ３０にログインする複数のクライアント７０とから構成されている。

【００１６】

図１を参照すると、認証サーバ２０は、認証手段２１と、ユーザ情報一覧テーブル２２とを含んで構成されている。

【００１７】

図３は、認証サーバ２０で管理しているユーザ情報一覧テーブル２２のデータ構造図を示す。ユーザ情報一覧テーブル２２には、ファイル管理サーバ３０にログインを許可されているユーザのユーザＩＤ（ＩＤｅｎｔｉｆｉｃａｔｉｏｎ），ユーザ名，パスワード，所属部署ＩＤ，所属部署名などからなるユーザ情報が登録されて一括管理されている。

【００１８】

図１を参照すると、ファイル管理サーバ３０は、データベース３１と、利用可能Ｗｅｂサーバ設置情報テーブル３２とを含んで構成されている。

【００１９】

データベース３１は、キャビネット，文書等のオブジェクトをツリー状に階層的に保持しており、各オブジェクトは、アクセス権情報（Ａ＊）（＊はワイルドカードであることを表す）を属性として持っている。各オブジェクト（インスタンス）は、データベース３１上で登録時に自動生成される一意なインスタンスＩＤを持っており、オブジェクトを指定するにはインスタンスＩＤが用いられる。インスタンスＩＤは、クライアント７０からファイル管理サーバ３０に、ユーザ情報（Ｐ１），および社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０のＩＰアドレス（ＩＰ１）とともに渡される。図１の例では、データベース３１は、”キャビネット”およびその配下に”文書Ｄ１”，”文書Ｄ２”，”文書Ｄ３”を含む。また、”文書Ｄ１”には、アクセス権情報Ａ１が属性として登録されている（他のオブジェクトも同様）。

【００２０】

図４を参照すると、アクセス権情報（Ａ＊）は、オブジェクト毎に１つの表で管理されて

おり、ユーザ情報（Ｐ＊）を用いた条件式の組み合わせ（ＡＮＤ条件，ＯＲ条件など）の形で設定が可能である。アクセス権情報（Ａ＊）は、要求元と、役職範囲と、設置情報と、アクセス権（参照権，更新権および削除権）の有無とを含む。要求元は、ユーザ，所属部署等を表す文字列である。役職範囲には、例えば、名前，所属部署名，勤務地，役職等が格納される。設置情報は、社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０のどちらを経由してファイル管理サーバ３０にログインしたかという条件（０で社内Ｗｅｂサーバ４０、１で社外Ｗｅｂサーバ６０）である。アクセス権（参照権，更新権および削除権）の有無は、理解しやすいように○や×として表記しているが、データベース３１上では数値として管理されている。

【００２１】

ファイル管理サーバ３０では、キャビネット，文書などの各オブジェクトに対する設定可能なアクセス権の種類として、参照権，更新権，削除権等が定義されている。例えば、クライアント７０からあるオブジェクトの参照が要求された場合、ファイル管理サーバ３０は、要求元のユーザが対象オブジェクトに対して参照権を有するかどうかを権利認証する。

【００２２】

ファイル管理サーバ３０は、社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０の設置情報をアクセス権情報の１つのカテゴリとして組み込むことにより、ユーザの対象オブジェクトへのアクセス時の権利認証の際には、経由した社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０の設置情報と適合するアクセス権情報（Ａ＊）のみが権利認証の対象となる（に切り分けられて判定される）。

【００２３】

図５は、利用可能Ｗｅｂサーバ設置情報テーブル３２のデータ構造を示す図である。利用可能Ｗｅｂサーバ設置情報テーブル３２は、ＩＰアドレスと、Ｗｅｂサーバがファイアウォール５０内外のどちらに設置されているかの設置情報（０でファイアウォール５０内、１でファイアウォール５０外）とがレコードとして、ファイル管理サーバ３０にログインする上で経由可能な社内Ｗｅｂサーバ４０および社外Ｗｅｂサーバ６０の数分だけ登録されている。ファイル管理サーバ３０は、ユーザ情報およびＩＰアドレスと、利用可能Ｗｅｂサーバ設置情報テーブル３２とに基づいてユーザのオブジェクトに対する権利認証を行う。

【００２４】

ファイル管理サーバ３０は、クライアント７０から渡される経由Ｗｅｂサーバのアドレス（ＩＰ１）のみでは、ファイアウォール５０内外のどちらに設置されているＷｅｂサーバを経由してログインしたかは判断できないので、ファイル管理サーバ３０の利用可能Ｗｅｂサーバ設置情報テーブル３２に設置情報をあらかじめ登録しておく。

【００２５】

図６を参照すると、認証サーバ２０におけるユーザ認証（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）処理は、ユーザＩＤ登録判定ステップＳ１０１と、パスワード正否判定ステップＳ１０２と、ユーザ情報返却ステップＳ１０３とからなる。

【００２６】

図７を参照すると、ファイル管理サーバ３０における権利認証（Ａｕｔｈｏｒｉｚａｔｉｏｎ）処理は、ＩＰアドレス登録判定ステップＳ２０１と、設置情報取得ステップＳ２０２と、オブジェクト存在判定ステップＳ２０３と、ユーザアクセス権有無判定ステップＳ２０４と、オブジェクト返却ステップＳ２０５とからなる。

【００２７】

次に、このように構成された第１の実施の形態に係るファイル管理システムにおけるアクセス制御方式の動作について説明する。

【００２８】

（１）　認証サーバ２０によるユーザ認証（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）について

【００２９】

ユーザは、ファイル管理サーバ３０のオブジェクトにアクセスする前に、クライアント７０から社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０を経由してファイル管理サーバ３０にログインする必要がある。ユーザは、通常、社内ネットワーク１０に接続されているクライアント７０からファイアウォール５０内に設置されている社内Ｗｅｂサーバ４０を経由してファイル管理サーバ３０にログインする。しかし、出張先や家庭などのクライアント７０からファイル管理サーバ３０にログインする場合には、ユーザは、ファイアウォール５０外に設置されている社外Ｗｅｂサーバ６０を経由した場合に限りファイル管理サーバ３０にログイン可能である。ただし、ユーザが社内から社外Ｗｅｂサーバ６０を経由してオブジェクトにアクセスすることは、ファイアウォール５０で制限されていない限りは可能である。

【００３０】

ユーザがクライアント７０から社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０を経由してファイル管理サーバ３０にログインする際に、認証サーバ２０によるユーザ認証が行われる。

【００３１】

詳しくは、ユーザは、クライアント７０のログイン画面からユーザＩＤおよびパスワードを入力し、ファイル管理サーバ３０へのログインを要求する。この際、クライアント７０と認証サーバ２０との通信が行われ、認証サーバ２０によるユーザ認証が行われる。なお、クライアント７０とファイル管理サーバ３０との通信が行われるのは、クライアント７０で、属性一覧の取得，更新画面での更新確定，キャビネット，フォルダなどの配下一覧の取得，対象の削除などの操作ボタンが押下された時点である。

【００３２】

認証サーバ２０は、まず、クライアント７０から受け取ったユーザＩＤがユーザ情報一覧テーブル２２に登録されているかどうかをチェックする（ステップＳ１０１）。ユーザＩＤが登録されていなければ、認証サーバ２０は、エラーをクライアント７０に返却する。

【００３３】

ユーザＩＤが登録されていたならば、認証サーバ２０は、クライアント７０から受け取ったパスワードがユーザ情報一覧テーブル２２にユーザＩＤと対応して登録されているパスワードと一致するかどうかをチェックする（ステップＳ１０２）。パスワードが一致しなかった場合、認証サーバ２０は、エラーをクライアント７０に返却する。

【００３４】

パスワードが一致した場合には、認証サーバ２０は、ユーザ情報一覧テーブル２２から該当ユーザのユーザ情報（Ｐ１）を取得してクライアント７０に返却し（ステップＳ１０３）、処理を終了する。

【００３５】

ファイル管理サーバ３０へのログインと同時にキャビネット一覧テーブル（図示せず）の取得が行われ、クライアント７０の画面には、通常、ユーザ固有のキャビネット一覧テーブルが表示される。キャビネット一覧テーブルに表示されているオブジェクトは、ログインしたユーザがアクセス権を有しているもののみであり、キャビネット一覧テーブルに表示されているのは各オブジェクトの一部の属性のみである。

【００３６】

（２）　ファイル管理サーバ３０における権利認証（Ａｕｔｈｏｒｉｚａｔｉｏｎ）

【００３７】

クライアント７０の画面にユーザ固有のキャビネット一覧テーブル（図示せず）が表示された後、ユーザがクライアント７０からオブジェクトへのアクセスを要求した場合、ファイル管理サーバ３０は、要求元のユーザがアクセス対象のオブジェクト（以下、対象オブジェクトという）のアクセス権を有するかどうかを権利認証する。

【００３８】

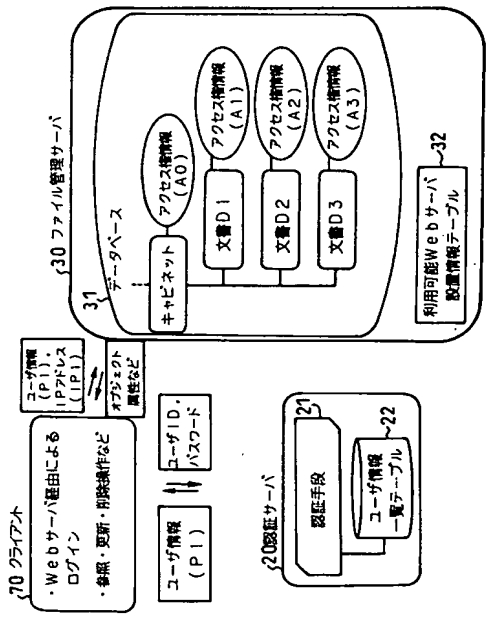
まず、クライアント７０は、対象オブジェクトを示すインスタンスＩＤを、認証サーバ２０から得られたユーザ情報，および社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０の

ＩＰアドレス（ＩＰ１）とともに、ファイル管理サーバ３０に渡す。
【００３９】
ファイル管理サーバ３０は、ユーザ認証で取得されたユーザ情報（Ｐ１）と、経由した社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０のＩＰアドレス（ＩＰ１）とを元に、対象オブジェクトに対するユーザの権利認証を行う。
【００４０】
ここで、ユーザＨ（ユーザ情報Ｐ１）が”文書Ｄ１”の参照を要求する場合を考える（図５参照）。”文書Ｄ１”には、要求元であるユーザＨに関して、図５に示すようなアクセス権情報（Ａ１）が属性として設定されているものとする。
【００４１】
クライアント７０で”キャビネット”配下のオブジェクト一覧を表示中（”文書Ｄ１”は一部の属性のみしか表示されていない）に、ユーザＨが”文書Ｄ１”の参照要求を行うと（参照ボタンを押下すると）、クライアント７０は、ユーザ情報（Ｐ１），および経由Ｗｅｂサーバ（社内Ｗｅｂサーバ４０または社外Ｗｅｂサーバ６０）のＩＰアドレス（ＩＰ１）をファイル管理サーバ３０に渡す。
【００４２】
ファイル管理サーバ３０は、まず、クライアント７０から渡された経由ＷｅｂサーバのＩＰアドレス（ＩＰ１）が、利用可能Ｗｅｂサーバ設置情報テーブル３２に登録されているかどうかを判定する（ステップＳ２０１）。
【００４３】
ＩＰアドレス（ＩＰ１）が利用可能Ｗｅｂサーバ設置情報テーブル３２に登録されていれば、ファイル管理サーバ３０は、経由ＷｅｂサーバのＩＰアドレスに対応する設置情報（０でファイアウォール５０内、１でファイアウォール５０外）を取得する（ステップＳ２０２）。
【００４４】
次に、ファイル管理サーバ３０は、インスタンスＩＤにより”文書Ｄ１”がデータベース３１上に存在するか否かをチェックする（ステップＳ２０３）。ファイル管理サーバ３０は、データベース３１上に存在するオブジェクトに対応する一覧テーブルを一括管理しており、インスタンスＩＤと一覧テーブルのデータとの比較処理を行う。
【００４５】
”文書Ｄ１”がデータベース３１上に存在する場合、ファイル管理サーバ３０は、要求元のユーザＨが”文書Ｄ１”の参照権を有しているかどうかの権利認証を行う（ステップＳ２０４）。詳しくは、ファイル管理サーバ３０は、まず、”文書Ｄ１”のアクセス権情報（Ａ１）を取得する。このとき、経由ＷｅｂサーバのＩＰアドレスが利用可能Ｗｅｂサーバ設置情報テーブル３２に登録されており、当該ＩＰアドレスに対応する設置情報が０と判定されたとすれば、ファイル管理サーバ３０は、「ユーザＨに対して参照および更新が可能」という条件のみが権利認証の対象となる。したがって、この場合、ファイル管理サーバ３０は、ユーザＨが”文書Ｄ１”の参照権および更新権を有することを判定する。
【００４６】
次に、ファイル管理サーバ３０は、データベース３１から文書Ｄ１およびその属性を取得し、クライアント７０へ返却する（ステップＳ２０５）。
【００４７】
クライアント７０は、ファイル管理サーバ３０から文書Ｄ１およびその属性を受信すると、これらを参照することができる。
【００４８】
なお、上記動作の説明では、アクセスが参照である場合を例にとって説明したが、アクセスが更新および削除の場合であっても、ほぼ同様の動作となることはいうまでもない。
【００４９】
また、オブジェクトを文書とした場合を例にとって説明したが、オブジェクトへのアクセス制御を、文書単位のみではなく、フォルダ単位やキャビネット単位でも行うことが可能

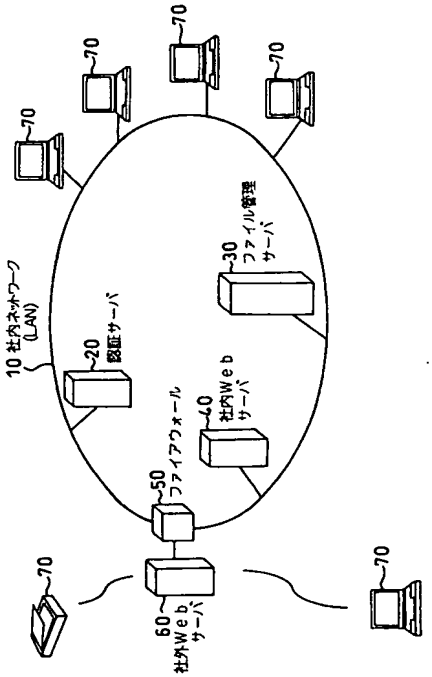
であることをいうまでもない。
【００５０】
このように、第１の実施の形態によれば、ファイル管理サーバ３０へのログイン時に経由したＷｅｂサーバが社内に存在するか社外に存在するかを加味して権利認証を行う仕組みを設けることにより、同一ユーザからの同一オブジェクトへのアクセスについても、社内からアクセスしたか社外からアクセスしたかに応じて権利認証を異ならしめることができる。例えば、同一ユーザからの同一オブジェクトへのアクセスに関して、参照は社内からでも社外からでも可能とする一方、更新は社内からでなければ許可しないようにすることが可能となる。
【００５１】
［第２の実施の形態］
図８は、本発明の第２の実施の形態に係るファイル管理システムにおけるアクセス制御方式の構成を示すブロック図である。本実施の形態に係るファイル管理システムにおけるアクセス制御方式は、図１に示した第１の実施の形態に係るファイル管理システムにおけるアクセス制御方式に対して、認証サーバ２０に認証サーバプログラム２００を備え、ファイル管理サーバ３０にファイル管理サーバプログラム３００を備えている点だけが異なっている。
【００５２】
認証サーバプログラム２００は、コンピュータである認証サーバ２０に読み込まれ、当該認証サーバ２０の動作を認証手段２１およびユーザ情報一覧テーブル２２として制御する。認証サーバプログラム２００の制御による認証サーバ２０の動作は、第１の実施の形態における認証サーバ２０の動作と全く同様になるので、その詳しい説明を割愛する。
【００５３】
また、ファイル管理サーバプログラム３００は、コンピュータであるファイル管理サーバ３０に読み込まれ、当該ファイル管理サーバ３０の動作をデータベース３１および利用可能Ｗｅｂサーバ設置情報テーブル３２として制御する。ファイル管理サーバプログラム３００の制御によるファイル管理サーバ３０の動作は、第１の実施の形態におけるファイル管理サーバ３０の動作と全く同様になるので、その詳しい説明を割愛する。
【００５４】
【発明の効果】
第１の効果は、アクセス権として設定可能な条件の幅を広げることにより、多様化するユーザの利用局面に対応したアクセス制御機能が提供できることである。その理由は、ファイル管理サーバへのログイン時に経由したＷｅｂサーバが社内に存在するか社外に存在するかを加味して権利認証を行う仕組みを設けるようにしたからである。
【００５５】
第２の効果は、それに伴いセキュリティ面での強化も図ることが可能であることである。その理由は、例えば、同一ユーザからの同一オブジェクトへのアクセスに関して、参照は社内からでも社外からでも可能とする一方、更新は社内からでなければ許可しないようにすることが可能であるからである。
【図面の簡単な説明】
【図１】本発明の第１の実施の形態に係るファイル管理システムにおけるアクセス制御方式の構成を示すブロック図である。
【図２】第１の実施の形態に係るアクセス制御方式が適用されるファイル管理システムのシステム構成図である。
【図３】図１中の認証サーバで管理されるユーザ情報一覧テーブルのデータ構造図である。
【図４】図１中のデータベースで管理されるアクセス権情報のデータ構造図である。
【図５】図１中の利用可能Ｗｅｂサーバ設置情報テーブルのデータ構造図である。
【図６】図１中の認証サーバにおけるユーザ認証処理を示すフローチャートである。
【図７】図１中のファイル管理サーバにおける権利認証処理を示すフローチャートである

。
【図８】本発明の第２の実施の形態に係るファイル管理システムにおけるアクセス制御方式の構成を示すブロック図である。
【符号の説明】
１０　社内ネットワーク
２０　認証サーバ
２１　認証手段
２２　ユーザ情報一覧テーブル
３０　ファイル管理サーバ
３１　データベース
３２　利用可能Ｗｅｂサーバ設置情報テーブル
４０　社内Ｗｅｂサーバ
５０　ファイアウォール
６０　社外Ｗｅｂサーバ
７０　クライアント
２００　認証サーバプログラム
３００　ファイル管理サーバプログラム
Ｓ１０１　ユーザＩＤ登録判定ステップ
Ｓ１０２　パスワード正否判定ステップ
Ｓ１０３　ユーザ情報返却ステップ
Ｓ２０１　ＩＰアドレス登録判定ステップ
Ｓ２０２　設置情報取得ステップ
Ｓ２０３　オブジェクト存在判定ステップ
Ｓ２０４　ユーザアクセス権有無判定ステップ
Ｓ２０５　オブジェクト返却ステップ

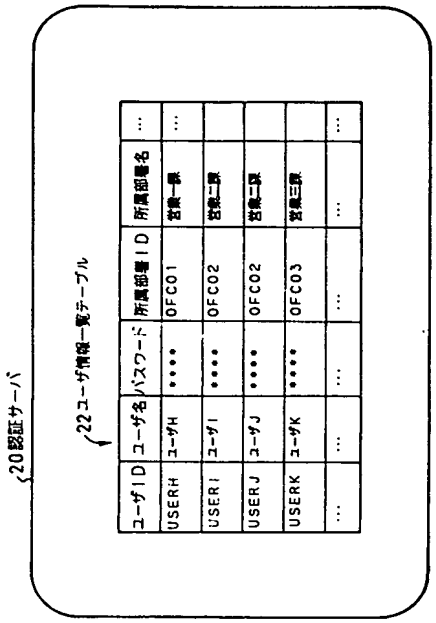
【図１】



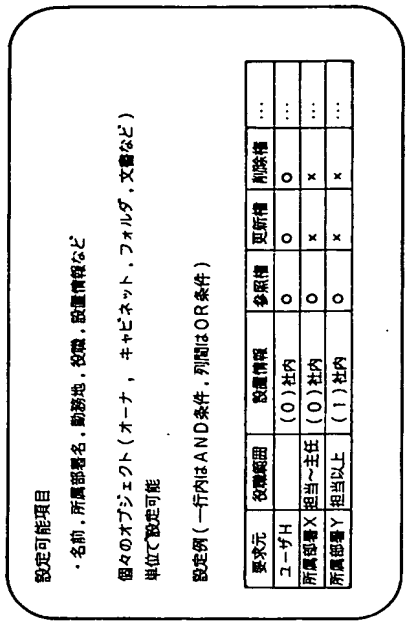
【図２】



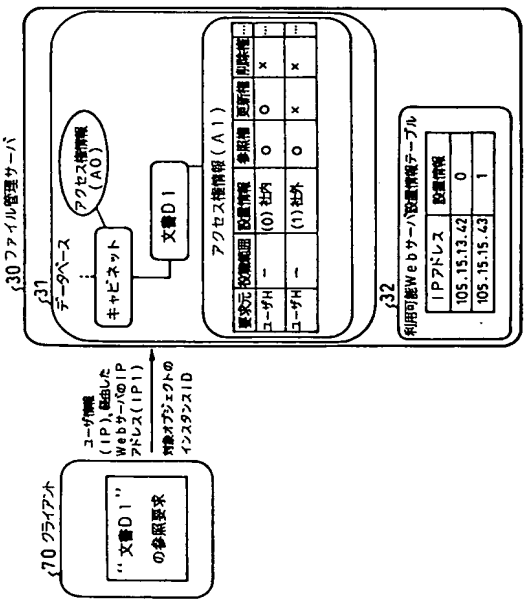
【図３】


20 認証サーバ
22 ユーザ情報一覧テーブル
ユーザID | ユーザ名 | パスワード | 所属部署ID | 所属部署名 | …
USERH | ユーザH | **** | OFC01 | 営業一課 | …
USERI | ユーザI | **** | OFC02 | 営業二課 |
USERJ | ユーザJ | **** | OFC02 | 営業二課 |
USERK | ユーザK | **** | OFC03 | 営業三課 |
… | … | … | … | … | …

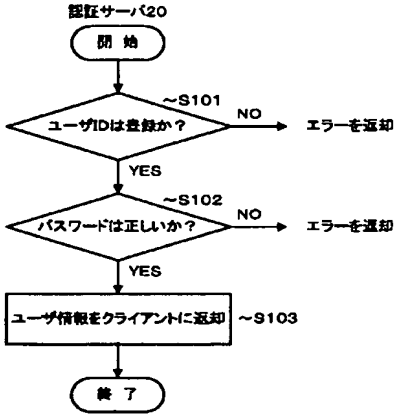
【図４】


アクセス権情報（A＊）
設定可能項目
・名前，所属部署名，勤務地，役職，設置情報など
個々のオブジェクト（オーナ，キャビネット，フォルダ，文書など）
単位で設定可能
設定例（一行内はAND条件，列間はOR条件）
要求元 | 役職範囲 | 設置情報 | 参照権 | 更新権 | 削除権 | …
ユーザH | | （0）社内 | ○ | ○ | ○ | …
所属部署X 担当～主任 | （0）社内 | ○ | × | × | …
所属部署Y 担当以上 | （1）社内 | ○ | × | × | …

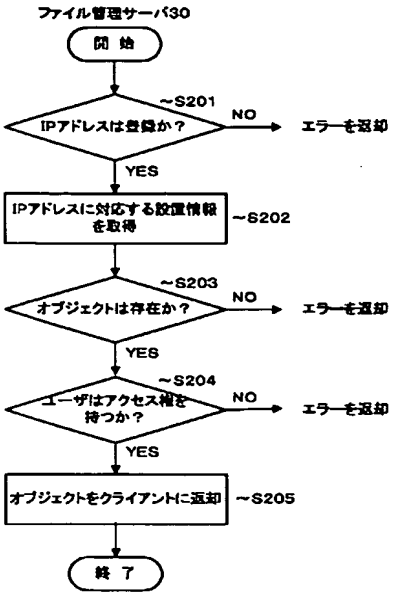
【図５】


30 ファイル管理サーバ
31
データベース
キャビネット
文書D1
アクセス権情報（A0）
アクセス権情報（A1）
要求元 | 役職範囲 | 設置情報 | 参照権 | 更新権 | 削除権 | …
ユーザH | ～ | （0）社内 | ○ | ○ | × | …
ユーザH | ～ | （1）社外 | ○ | × | × | …
32
利用可能Webサーバ設置情報テーブル
IPアドレス | 設置情報
105.15.13.42 | 0
105.15.15.43 | 1
70 クライアント
“文書D1”の参照要求
ユーザ情報（IP），接続したWebサーバのIPアドレス（IP1）
対象オブジェクトのインスタンスID

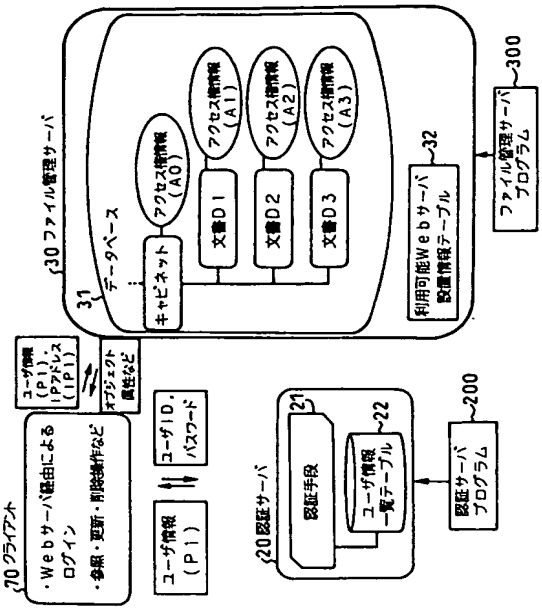
【図６】


認証サーバ20
開始
S101
ユーザIDは登録か？
NO
エラーを返却
YES
S102
パスワードは正しいか？
NO
エラーを返却
YES
ユーザ情報をクライアントに返却
S103
終了

【図７】


ファイル管理サーバ30
開 始
IPアドレスは登録か？
~S201
NO
エラーを返却
YES
IPアドレスに対応する設置情報を取得
~S202
オブジェクトは存在か？
~S203
NO
エラーを返却
YES
ユーザはアクセス権を持つか？
~S204
NO
エラーを返却
YES
オブジェクトをクライアントに返却
~S205
終 了

【図８】


30 ファイル管理サーバ
31
データベース
キャビネット
アクセス制御情報 (A0)
アクセス制御情報 (A1)
アクセス制御情報 (A2)
アクセス制御情報 (A3)
文書D1
文書D2
文書D3
32
利用可能Webサーバ設置情報テーブル
ファイル管理サーバプログラム
300
ユーザ情報 (P1) IPアドレス (IP1)
オブジェクト属性など
10 クライアント
・Webサーバ経由による ログイン
・参照・更新・削除操作など
ユーザID, パスワード
ユーザ情報 (P1)
20 認証サーバ
21
認証手段
22
ユーザ情報一覧テーブル
認証サーバプログラム
200